BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-119

1 MARCH 1999

Communications and Information

ELECTRONIC MAIL (E-MAIL) MANAGEMENT AND USE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/GCOM (MSgt Robert Cole) Certified by: HQ USAF/SCXX (Lt Col L. Wilson)
Supersedes AFI 33-119, 1 March 1997. Pages: 29
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*, and establishes electronic mail (E-mail) manager and user duties and responsibilities. It provides rules, standards, and guidance relating to the use of E-mail by the Air Force. This instruction applies to all uses of AF E-mail systems by AF organizations, personnel, and contractors regardless of the classification of the information transmitted or received. Failure to observe the prohibitions and mandatory provisions of paragraphs **3.1.** and **3.3.** and its subparagraphs by military personnel is a violation on Article 92, Uniform Code of Military Justice (UCMJ). Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/XPXP), 203 West Losey Street, Room 1060, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/GCO, 203 West Losey Street, Room 3065, Scott AFB IL 62225-5222. Refer to **Attachment 1** for a glossary of references and supporting information. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed. This revision updates the entire instruction. Paragraph **2.** includes establishing organizational and individual E-mail accounts. Paragraph **3.** differentiates between acceptable and unacceptable use of E-mail. Paragraph **4.** includes a reference to "//SIGNED//" in the signature blocks. Paragraph **5.** includes standard naming conventions for Air Force-owned and maintained messaging systems and Air Force-operated Defense Messaging System equipment. The (|) preceding the title indicates a major revision from the previous edition.

1. Scope. This instruction lists responsibilities for users and managers of Air Force electronic messaging and mail systems. It sets forth policies regarding the official or authorized use of government-provided E-mail communications systems. In the context of this instruction, E-mail and electronic messaging are considered synonymous. E-mail is used to supplement or replace traditional mail (Base Information Transfer System [BITS], US Postal Service, and other commercial mail services), facsimile, telephone, and other messaging systems.

2. Roles and Responsibilities.

2.1. HQ USAF/SC establishes AF policy for E-mail administration and use. E-mail policies include planning, acquisition, maintenance, use, formats, E-mail address naming conventions, access, privacy, security, records management, and training responsibilities.

2.2. Air Force Functional Managers will:

2.2.1. Comply with HQ USAF/SC policy and as required, identify and establish any additional or more restrictive policies for E-mail administration and use within their programs.

2.2.2. Determine the extent the function will use E-mail.

2.2.3. Consult Department of Defense (DoD) 5200.1-R, *DoD Information Security Program*, to determine the level of protection that is required for functional information sent by Air Force E-mail.

2.3. Major Commands (MAJCOM), Direct Reporting Units (DRU), and Field Operating Agencies (FOA) will:

2.3.1. Disseminate and implement Air Force E-mail policy within their organizations.

2.3.2. As required, identify and establish any additional or more restrictive policies for E-mail administration and use within their organizations, and include Air Force Functional Manager policies associated with their programs.

2.4. Wing, Wing-Level Equivalents, and Tenant Organizations will:

2.4.1. Ensure compliance with Air Force and MAJCOM E-mail policy within their organizations.

2.4.2. As required, identify and establish any additional or more restrictive policies for E-mail administration and use within their organizations. Coordinate additional or more restrictive policies with their MAJCOM or DRU/FOA headquarters.

2.5. Wing Commanders will:

2.5.1. Order periodic inspections of stored E-mail communications on those E-mail systems under their command to ensure compliance with E-mail policy.

2.5.2. Commanders should coordinate with their servicing legal office prior to ordering a periodic inspection of stored E-mail communications to ensure the inspection meets required criteria for an inspection under Military Rule of Evidence 313.

2.6. Commanders at all levels will:

2.6.1. Ensure E-mail users within their command are educated and trained on the appropriate use of E-mail according to this AFI and other applicable Air Force policy. Training will include:

2.6.1.1. Security.

2.6.1.2. Information Security.

2.6.1.3. Operational Security.

2.6.1.4. System Security.

2.6.1.5. Personnel Security.

2.6.1.6. Professional Courtesies.

2.6.1.7. Information Protection Security Awareness.

2.6.1.8. Local Operating Procedures.

2.6.1.9. User Responsibilities.

2.6.1.10. Records Management Requirements.

2.6.1.11. Authorized Use.

2.6.1.12. Unauthorized Use.

2.6.1.13. Systems Operations and Capabilities.

2.6.1.14. Privacy Act.

2.6.1.15. Public Release of Information and Freedom of Information Act (FOIA).

2.6.2. Ensure internal storage and control of E-mail is consistent with Air Force information security and records management policies.

2.6.3. Ensure procedures are in place to disable and/or remove accounts and file permissions within 24 hours of an individual's departure on a permanent change of station (PCS).

2.7. E-mail Administrators (typically System or Workgroup Administrators or Network Managers) will:

2.7.1. Implement Air Force E-mail policy.

2.7.2. Manage the day-to-day operations of the assigned Air Force E-mail systems and act as the primary points of contact for E-mail policy implementation.

2.7.3. Implement Air Force and Defense Information Systems Agency (DISA) electronic messaging registration procedures according to AFI 33-127, *Electronic Messaging Registration and Authority*.

2.7.4. When directed by the commander authorized to do so, periodically inspect stored communications to ensure compliance with Air Force E-mail policy.

2.7.4.1. Administrators will protect the confidentiality of the contents of E-mail communications viewed during periodic inspections.

2.7.4.2. Administrators will report any evidence of criminal activity inadvertently discovered during periodic inspections to the commander concerned or to appropriate law enforcement authorities.

2.8. E-mail Users will:

2.8.1. Comply with the Air Force and MAJCOM E-mail policies.

2.8.2. Maintain responsibility for the content of their E-mail messages and ensure that messages they send meet Air Force directives regarding acceptable use of E-mail (see paragraph **3.3.**).

2.8.3. Maintain sent and received information according to Air Force records management directives: Air Force Manual (AFMAN) 37-123, *Management of Records* (will convert to AFMAN 33-323); AFI 37-138, *Records Disposition, Procedures and Responsibilities* (will convert to AFI 33-338); and AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339). See paragraph **8.** for more detailed records management guidance.

2.8.4. Make sure the account from which the E-mail message was sent is clearly identified in the "FROM" element of the E-mail header, the "BODY" of the message, or both. E-mail senders will not use anonymous accounts or forwarding mechanisms that purposely attempt to conceal the originator of a message unless approved by the commander for the purposes of soliciting anonymous feedback.

2.8.5. Get approval from their chain of command before subscribing to or participating in E-mail list-servers and news groups except official Air Force internal information products. These products are managed and approved by Air Force Public Affairs (SAF/PA) and accessible from Air Force Link (http://www.af.mil). This policy recognizes that list-servers are a potentially valuable

information tool for E-mail users; however, the potential for abuse is high. Approve each list-server individually. Blanket approval for user participation in all list-servers is not appropriate.

2.8.6. Report any suspected violations of E-mail policy to their supervisor, information protection office, or E-mail administrator.

2.8.7. Verify the authenticity of messages received if the authenticity of the message is uncertain.

3. E-mail Policy.

3.1. General. Air Force members and employees use government communications systems with the understanding that any type of use, authorized or unauthorized, incidental or personal, serves as consent to monitoring. Members of the Air Force or civilian employees may use a government-provided E-mail communications system only for official or authorized use. Any other use is prohibited. Military members who fail to observe this prohibition may be subjected to disciplinary action under Article 92 of the Uniform Code of Military Justice. Civilian employees who violate this prohibition may face administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

3.1.1. E-mail is subject to the requirements of the Freedom of Information Act and the Privacy Act of 1974. (See paragraph **9.** for additional guidance.)

3.1.2. Use caution when sending E-mail to a large number of recipients. Digital images as well as mass distribution of smaller messages may delay other traffic, overload the system, and subsequently cause system failure.

3.1.3. Use caution when sending an E-mail message to mail distribution lists. Use electronic bulletin boards or E-mail public folders for nonmission-related E-mail (e.g., 'Car Wash'). Imprudent use of address lists clogs E-mail accounts and often clutters in-boxes.

3.2. Official E-mail Communications. Use E-mail to transmit both organizational and individual correspondence. E-mail account users bear sole responsibility for material they access and send via E-mail.

3.2.1. Coordination and Staffing. Using E-mail for coordination and staffing increases efficiency when properly managed. Use organizational accounts when sending correspondence to offices for coordination or action. Local commanders may supplement this policy according to local conditions and operating procedures. Users are responsible for proper coordination and staffing of E-mail in accordance with this AFI and local directives.

3.2.2. Transmitting Official Taskings. Use E-mail systems to transmit official taskings. Send official taskings from an individual or organizational E-mail account to an organizational E-mail address.

3.2.2.1. It is the sender's responsibility to make sure taskings are received by the intended receiver.

3.2.2.2. It is the receiver's responsibility to ensure the accuracy of the tasking.

3.2.3. Organizational E-mail.

3.2.3.1. All USAF organizations with E-mail capability will establish organizational E-mail

accounts. Use organizational E-mail to replace or supplement formal Air Force formats for communications like official memorandums, messages, orders, taskings, or letters. This includes messages and other communications exchanged between organizational elements in support of command and control, combat support, combat service support, and other functional activities. Typically, these messages provide formal direction, establish a formal position, commitment, or response for the organization.

3.2.3.2. Organizational E-mail accounts will use the Air Force standard organizational abbreviations and standard Air Force office symbols as the "UserID" (see paragraph **5.** and **Attachment 6** for detailed guidance).

3.2.3.3. Each office will designate an individual or individuals to monitor the organization's mailbox regularly to ensure messages requiring action are acted upon promptly. Each individual should have a unique identifier that the system can authenticate and provide an audit trail. When E-mail systems cannot provide a unique identifier, use administrative procedures to provide the audit trail.

3.2.3.4. Establish, at a minimum, separate organizational E-mail accounts for wing commanders, vice wing commanders, senior enlisted advisors, group commanders, squadron commanders, and staff agencies.

3.2.3.5. Establish, at a minimum, separate organizational E-mail accounts down to the division level at higher headquarters. This includes, but is not limited to, centers, numbered air forces, MAJCOMs, FOAs, DRUs, HQ USAF, and the Air Force Secretariat.

3.2.4. Individual E-mail.

3.2.4.1. Provide accounts for Air Force personnel at locations where the capability exists and where deemed appropriate to facilitate Air Force communications unless specifically prohibited by law, policy, contract, or other binding agreement.

3.2.4.2. Individual E-mail includes working communications between individual DoD personnel within administrative channels, both internal and external to the specific organizational element, including non-DoD users. It replaces or supplements telephone calls, notes, or work-related communications between individuals. Such messages do not generally commit or direct an organization.

3.2.4.3. Individual E-mail accounts will use the Air Force standard syntax (UserID@domain) to identify the account owner. See paragraph **5.** for specific guidance.

3.3. Official-Use, Authorized Use, and Use of Subscription Services. Air Force E-mail systems are provided to support the Air Force mission. Use E-mail systems only for official uses or for authorized personal use as explained below. For military members, failure to observe the provisions in paragraphs **3.3.1.** and **3.3.2.** constitutes a violation of Article 92, UCMJ. Civilian employees who fail to observe the provisions in paragraphs **3.3.1.** and **3.3.2.** may face administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions.

3.3.1. Official Use. Official use includes communications, including emergency communications, the Air Force has determined necessary in the interest of the Federal government. Official use includes, when approved by the theater commander in the interest of morale and welfare, those communications by military members and other Air Force employees who are deployed for extended periods away from home on official business.

3.3.1.1. The following do not constitute official use of governmental communications systems and are prohibited.

3.3.1.1.1. Distributing copyrighted materials by E-mail or E-mail attachments without consent from the copyright owner. Failure to maintain consent may violate federal copyright infringement laws and could subject the individual to civil liability or criminal prosecution.

3.3.1.1.2. Sending or receiving E-mail for commercial or personal financial gain using government systems.

3.3.1.1.3. Intentionally or unlawfully misrepresenting your identity or affiliation in E-mail communications.

3.3.1.1.4. Sending harassing, intimidating, abusive, or offensive material to, or about others.

3.3.1.1.5. Using someone else's identity (UserID) and password without proper authority.

3.3.1.1.6. Causing congestion on the network by such things as the propagation of chain letters, broadcasting inappropriate messages to groups or individuals, or excessive use of the data storage space on the E-mail host server.

3.3.2. Authorized Personal Use. An Agency Designee is the first supervisor in the chain of command who is a commissioned officer or a government civilian holding a rank of General Schedule-11 (GS-11), or above. An agency designee may authorize limited personal use of government-provided E-mail communication, when it:

3.3.2.1. Serves a legitimate public interest,

3.3.2.2. Conforms with theater commander-in-chief (CINC) and MAJCOM policies,

3.3.2.3. Does not adversely affect the performance of official duties,

3.3.2.4. Is of reasonable duration and frequency, and whenever possible, is made during personal time (such as after-duty hours or lunch time),

3.3.2.5. Does not overburden the communications system with large broadcasts or group mailings,

3.3.2.6. Does not create significant additional costs to DoD or the Air Force, and

3.3.2.7. Does not reflect adversely on DoD or the Air Force (such as uses involving pornography, chain letters, unofficial advertising, soliciting or selling, violations of statute or regulation, inappropriately handled classified information or other uses that are incompatible with public service).

3.3.2.8. Examples of authorized limited personal use include, but are not limited to:

3.3.2.8.1. Brief communications made while traveling on official business to notify family members of official transportation or schedule changes.

3.3.2.8.2. Using government systems to exchange important and time-sensitive information with a spouse or other family members; such as, scheduling doctor, automobile, or home repair appointments, brief internet searches, or sending directions to visiting relatives.

3.3.2.8.3. Educating or enhancing the professional skills of employees (e.g., use of communication systems, work-related application training, etc.)

3.3.2.8.4. Improving the morale of employees stationed away from home for extended periods.

3.3.2.8.5. Job searching in response to Federal government downsizing.

3.3.3. Subscription Services. Internet E-mail access grants users the ability to subscribe to a variety of list servers, mailing lists, and discussion groups. These services may include professional news groups sponsored by Air Force agencies and other news groups sponsored by non-Air Force agencies, including the DoD, other Federal agencies, educational institutions, and commercial activities.

3.3.3.1. Air Force personnel may subscribe to official Air Force-sponsored list servers, mailing lists, and discussion groups. Participation in other mailing lists and discussion groups requires written approval of the cognizant authority before subscribing to such information sources. Recommended approval levels are unit commanders at base-level and division chiefs at headquarters. Any person using government equipment to participate in any news group or list-server, Air Force-sponsored or not, must clearly state "The opinions expressed are those of the individual and do not represent an official position of the United States Air Force."

3.3.3.2. When an extended absence will not allow access to your E-mail account, unsubscribe or suspend mail from any mailing lists or list-servers. This will alleviate large backlogs of received messages that consume expensive server storage resources. Remember, some discussion lists and Usenet groups have members from many foreign countries and discussions in these groups may lead to inadvertent disclosure of sensitive information. See paragraph **9.** for security instructions.

3.3.3.3. Participation in news groups or list-servers whose content is contrary to the standards set by the *Joint Ethics Regulation* (e.g., obscene, offensive, etc.) is prohibited. Commanders may direct E-mail administrators to set up permanent blocks on a specific site, news group or list-server address to prevent subscription to such services.

3.3.3.4. Users are responsible for protecting Air Force information, which includes both sensitive information and classified data.

4. Formats.

4.1. Official Signatures on E-mail. Organizational E-mail includes official communications such as memorandums (letters), notes, messages, reports, and so forth, and will follow specific formats found in this instruction and Air Force Handbook (AFH) 33-337, *The Tongue and Quill*. All official E-mail will include "//SIGNED//" in upper case before the signature block to signify it contains official Air Force information (e.g., instructions, directions, or policies).

4.2. Senders will include a formal signature block on all organizational E-mail. For example:

//SIGNED//
LARRY D. WILSON, Lt Col, USAF
Chief, Policy Division
Directorate of Policy and Resources

4.3. Individual E-mail typically uses a less formal writing style, but is still considered official when the sender is acting in an authorized capacity and includes "//SIGNED//" before the signature block. For example:

//SIGNED//
LARRY D. WILSON, Lt Col, USAF
Chief, Policy Division

5. Naming Conventions.

5.1. Implement E-Mail naming conventions in accordance with this AFI and the Joint Technical Architecture-Air Force (JTA-AF) Version 1.5, section 4.1.9 and the Standard Air Force Electronic Mail (E-Mail) Naming Conventions brochure. The brochure (located on the JTA-AF home page at http://www.afca.scott.af.mil/jta-af/) contains expanded descriptions and details on all Air Force E-Mail naming conventions. These individual, organization, and display naming conventions are mandatory for those systems that can technologically support them. Organizations have until 1 January 2002 to comply with these standards.

5.2. The standard format for "individual" SMTP addresses is: "FIRSTNAME.LASTNAME@BASE.AF.MIL" (e.g., john.smith@scott.af.mil). Hyphenated names remain hyphenated with a period between the first and last name (e.g., mary.jones-daniel@scott.af.mil). Add a period and a number as needed to specifically identify users with similar names within domains (e.g., john.smith1@scott.af.mil). Apostrophes in names are not permitted (e.g., scott.ogrady@hill.af.mil).

5.3. The standard Air Force individual display naming convention is LAST NAME, FIRST NAME, MIDDLE INITIAL, GENERATION QUALIFIER, RANK, ORGANIZATION, AND OFFICE. The elements are separated by a space. Punctuation (including commas) is not permitted between the elements. The syntax is: <LASTNAME FIRSTNAME MIDDLEINITIAL GENERATIONQUALIFIER RANK ORGANIZATION/OFFICE. For example, "Telles Gabriel H Jr Maj USAF/SCXX." Use "CONTRACTOR" in the rank field to identify vendors and contractors. If a tiebreaker is needed, spell out the middle name.

5.4. The standard format for the SMTP organizational naming convention is: "ORG.OFFICE@BASE.AF.MIL" (e.g., afcic.xpx@pentagon.af.mil). You may add additional information to accommodate other units such as detachments and operating locations (see **Attachment 6**).

5.5. The standard Air Force organizational display naming convention is STANDARD ORGANIZATIONAL ABBREVIATION, STANDARD AF OFFICE SYMBOL, AND SHORT DESCRIPTION. The first two elements are separated by a slash, and the description elements are separated by a space. The syntax is: <ORGANIZATIONAL ABBREVIATION/OFFICE SYMBOL SHORT DESCRIPTION OF OFFICE> (e.g., ACC/SE Safety Office). Obtain the standard organizational abbreviation from AFDIR 37-135, *Air Force Address Directory* (converted to a database at http://afdir.hq.af.mil/afdir/index.cfm). Obtain the standard Air Force office symbol from AFMAN 37-127, *Air Force Standard Office Symbols* (will convert to AFMAN 33-327).

5.6. For nonstandard systems limited to an eight-character UserID, maintain current E-Mail address format until migration to a system that can support this standard.

5.7. Refer to **Attachment 6** for additional descriptions and details on **Air Force** E-Mail naming conventions.

6. Authentication.

6.1. Take special care to prove the identity of a person or organization initiating an electronic transaction. To authenticate an E-mail message, you must prove its origin. Authentication does not necessarily require a digital signature. You may consider E-mail authentic because a user log-on and password are used to gain access to the mail system before the message is sent. However, the recipient can make full authentication of normal E-mail by contacting the sender to confirm the originator sent the message.

6.2. The next level of authentication above the generic E-mail system security involves the use of digital signatures. A digital signature shows that the person who signed the document had access to the proper key and the password for the key as indicated by the signature. It also confirms the document was not modified since it was signed.

7. Effective Electronic Communications. Air Force personnel follow certain courtesies and conventions when communicating via memorandum or telephone. Similar courtesies and conventions apply to electronic communications; you should use these conventions to compose and disseminate information via E-mail.

7.1. Professional Courtesies. Extend the professional courtesies below to individuals or groups as applicable.

7.1.1. Individuals will:

7.1.1.1. Follow the chain of command when sending messages up the chain of command as you would using any other medium. Send courtesy copies as necessary.

7.1.1.2. Focus on one subject per message and always include a pertinent subject title for the message; this helps the user to locate the message quickly later on.

7.1.1.3. Include your signature block at the bottom of E-mail messages when needed to ensure all recipients can identify the originator.

7.1.1.4. Be professional and careful whenever you write about others. Understand that E-mail is easily forwarded; and messages intended to be private or personal may not remain so. Material sent via E-mail is not secure, and may be subject to monitoring and retransmittal.

7.1.1.5. Use a tone of address that is appropriate to the recipient.

7.1.2. It is preferable to reference the source of a document and provide instructions on how to get a copy.

7.1.3. When replying to a discussion group message, check the address to make sure it is going to the intended location (person or group). It can be very embarrassing to reply incorrectly and post a personal message to an entire discussion group that was intended for only one individual.

7.1.4. The use of automatic response (e.g.,, “I’m out of the office”) messages is discouraged because list-servers and mail reflectors react poorly to these types of messages.

7.1.5. Summarize the conversation up front if you forward an E-mail containing a long string of replies.

7.2. Effective Writing.

7.2.1. Make your most important main point in the first sentence or paragraph.

7.2.2. Use the basic elements of effective writing: clarity, brevity, and courtesy.

7.2.3. Delete outdated or unwanted information from outgoing messages.

7.2.4. Edit messages for spelling and grammatical errors.

7.2.5. Use acronyms or abbreviations when feasible. However, senders should recognize that messages filled with acronyms and abbreviations are confusing and annoying to the reader. Use acronyms and abbreviations that are of a common-use-nature, and understood by the intended audience. "Spell out" acronyms and abbreviations the first time they are used in the document.

7.2.6. Capitalize words only to highlight an important point or to distinguish a title or heading. You can also use *asterisks* surrounding a word to make a stronger point. Capitalizing whole words which are not titles is generally considered SHOUTING. Do not SHOUT unless you must emphasize a particular point.

7.2.7. Cite all quotations, references, and sources.

7.2.8. Do not use unprofessional language and limit the use of sarcasm and humor. Without face-to-face communications, the recipient may view your "joke" as criticism.

8. Records Management.

8.1. Legal Authority. The Federal Records Act requires the Air Force to identify and preserve records including records created or received on E-mail systems.

8.2. E-mail messages. Maintain E-mail that contains information that serves as adequate and proper documentation of the organization's functions, policies, decisions, procedures, and transactions.

8.3. Determining Record Status. E-mail messages are records when they meet both of the following conditions:

8.3.1. They are made or received by an agency of the United States Government under federal law or in connection with the transaction of agency business.

8.3.2. They are preserved, or are appropriate for preservation, as evidence of the agency's or organization's activities, or because of the value of the information they contain.

8.4. Management and Disposition. You must systematically manage, store, and then destroy E-mail records, like federal records in any other media after their usefulness has expired.

8.4.1. Management Rules:

8.4.1.1. Preserve the content, context, and structure of records in a useable format for their authorized retention period. A complete E-mail record will include the message itself, attachments (e.g., word processing and other electronic documents transmitted with the message), and transmission data (e.g., originator, recipients, addresses, date, and time).

8.4.1.2. Make records easily accessible by individuals who have a business need to access them.

8.4.1.3. Arrange E-mail records in accordance with the approved file plan.

8.4.1.4. Preserve E-mail system and transmission data that identifies users by codes, nicknames, addresses, and distribution lists to ensure you can identify the originator and recipients of record messages.

8.4.1.5. Preserve receipts and acknowledgments that show delivery and disposition status (e.g., delivered, opened, replied, deleted, etc.) of a message. Maintain them with the original official E-mail record (see paragraph **3.2.2.1.**).

8.4.1.6. Ensure federal records sent or received on E-mail systems outside organizational control are preserved. Ensure reasonable steps are taken to capture available transmission and receipt data needed by the agency for record-keeping purposes.

8.4.2. On-Site and Off-Site Storage.

8.4.2.1. Get approval for any electronic system used for record-keeping purposes from the local records manager.

8.4.2.2. Store record copies of E-mail messages in systems designed as record-keeping systems.

8.4.2.3. When an E-mail record is retained in a record-keeping system, you may delete the E-mail message from the E-mail system.

8.4.2.4. Keep selected archived E-mail files required for system reconstitution after catastrophic system failure in a secure area and physically separated from the network control center (NCC) E-mail server. Select the off-site storage location based on its distance from the NCC E-mail server, the temperature and humidity, and the physical security of the building. Place a priority schedule for recreating files at the off-site storage location.

8.4.3. Destruction.

8.4.3.1. Protect records from unauthorized or unintentional disclosure or destruction (see paragraph **8.**).

8.4.3.2. Destroy in accordance with AFMAN 37-139 (will convert to AFMAN 33-339).

9. Security.

9.1. General. Electronic communications such as E-mail messages are primarily delivered to their destinations via the unprotected or nonencrypted internet. You can route E-mail messages from their origin through many internet communications nodes to a destination. Interception of the information can occur at any point along the way. To prevent unauthorized disclosure of information, determine the level of security measures required by the sensitivity of the data and implement sufficient access and security controls to protect it. The information below describes programs and measures to help protect information from unauthorized disclosure. It also lists some information considered as sensitive information which requires safeguards.

9.2. Policy. The following paragraphs cite DoD policies:

9.2.1. Safeguard classified and sensitive information at all times. Apply safeguards so information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required by Office of Management and Budget (OMB)/ Information Security Oversight Office (ISOO) Directive No. 1, *Classified National Security Information;* DoD 5200.1-R, *Information Security Program*, AFI 31-401; *Information Security Program Management*, and supplemental guidance thereto.

9.2.2. Safeguard all unclassified information to prevent tampering, loss, destruction, fraud, waste, and abuse. This is necessary to protect the DoD investment in obtaining and using information.

9.2.3. Safeguard information and E-mail system resources against sabotage, denial of service, espionage, misappropriation, misuse, or release to unauthorized persons. Continually employ administrative, procedural, physical, environmental, personnel, communications, emanations, operations, information, and computer security safeguards.

9.2.4. Ensure the mix of safeguards selected for E-mail systems that process classified or sensitive information meets the minimum requirements as set forth in DoD Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AIS)*, Enclosure 3. Meet these minimum requirements through automated and manual means in a cost-effective and integrated manner. Use DoDD 5200.28, Enclosure 4, to identify any additional requirements over and above the set of minimum requirements.

9.2.5. DoD military, civilians, or contractor personnel using unclassified automated information systems that have access to sensitive information must possess, at a minimum, a National Agency Check or Entrance National Agency Check in accordance with DoD 5200.2-R, *Personnel Security Program*, or screening in accordance with AFI 31-501, *Personnel Security Program Management*. Those personnel requiring access to classified systems are subject to the appropriate investigation.

9.3. Operations Security (OPSEC). Users of E-mail systems must constantly stay aware of communications systems vulnerabilities and the need to safeguard critical information, OPSEC indicators, and other sources of information. As a minimum, you must encrypt critical information, OPSEC indicators, and other sources of information before sending it across the internet. For additional guidance on OPSEC requirements see AFI 10-1101, *Operations Security*.

9.4. Sensitive Information.

9.4.1. Identification of Critical Information. Critical information is information about friendly force's (US, allied, and coalition) activities, intentions, capabilities, and limitations. You can derive critical information from bits and pieces of related information (indicators) that are almost always available to the trained eye. It usually takes only a few key items of critical information to develop an accurate understanding of friendly force's plans and objectives. An adversary uses the information to gain military, political, diplomatic, and technological advantages. Inadvertent release of critical information could reduce mission effectiveness (e.g., disclosure of time over target), lead to mission failure (e.g., canceling a sortie), cause severe damage to friendly forces (e.g., divulge force locations), or cause loss of lives.

9.4.2. Privacy Act Information. The Privacy Act of 1974 provides safeguards to protect individuals against an invasion of personal privacy. As such, the electronic collection, maintenance, use, and dissemination of personal information directly affect the privacy of an individual. Protect the privacy of individuals. Use an appropriate level of protection to prevent unintentional or unauthorized disclosure when sending Privacy Act information across the internet. Follow the procedures in AFI 37-132, *Air Force Privacy Act Program* (will convert to AFI 33-332), to safeguard Privacy Act information. The following items of information are examples of information normally protected from disclosure: Social Security Number (SSN); marital status; number or sex of dependents; gross salary of military personnel; civilian educational degrees and major areas of study; school and year of graduation; home address or phone number; age or date of birth; present or

future assignments for overseas, or for routinely deployable or sensitive units; and office, unit address, and duty phone for overseas, or for routinely deployable or sensitive units.

9.4.2.1. SSNs are personal and unique for each individual and you must protect them as For Official Use Only (FOUO) per AFI 37-131, *Freedom of Information Act Program* (will convert to DoD 5400.7-R/AF Supplement). Use an appropriate level of protection to prevent unintentional or unauthorized disclosure when sending SSNs across the internet.

9.4.3. Freedom of Information Act (FOIA). The Air Force discloses its records to the public in accordance with the FOIA. Some records are exempt from release if the release would cause identifiable harm. The following categories of information are normally exempt from routine disclosure and you must protect them from unintentional or unauthorized disclosure: classified information; internal personnel rules or practices; information specifically exempted from disclosure by another statute; confidential commercial information; inter- or intra-agency record that is in deliberation or is predecisional in nature; information whose disclosure would constitute an invasion of privacy; records or information compiled for law enforcement purposes. Do not send information normally exempt under FOIA across the internet without an appropriate level of protection to prevent unintentional or unauthorized disclosure. Refer to AFI 37-131 for additional guidance.

9.4.4. Protection of E-mail Addresses. To reduce the risk of attack on Air Force E-mail systems, do not indiscriminately release E-mail addresses. Lists of individual and organizational E-mail addresses are exempt from disclosure under the FOIA as internal information, the disclosure of which would risk circumvention of a regulation (FOIA Exemption 2). Reference AFI 33-129, *Transmission of Information Via the Internet*, for guidance on the inclusion of E-mail addresses in Web Pages.

9.4.5. Physical Security. The E-mail system administrator must set up procedures defining the control, security, access, and maintenance of all E-mail storage media.

9.4.6. Off-site Storage. Keep archived E-mail files as necessary for system reconstitution after catastrophic system failure in a secure area and physically separated from the NCC E-mail server. Select the off-site storage location based on its distance from the NCC E-mail server, the temperature and humidity, and the physical security of the building. Place a priority schedule for recreating files at the off-site storage location.

9.4.7. E-mail Access. Access by foreign nationals to US Government-owned or US Government-managed automated information systems is authorized only by the DoD component head. Access must remain consistent with the DoD, the Department of State, and the Director of Central Intelligence Agency policies and when applicable, government-to-government agreements or memorandums of understanding. Reference DoDD 5200.28.

9.5. Handling Classified E-mail. Network and E-mail administrators must possess a security clearance equal to the highest security classification of the information riding the network they administer.

9.5.1. Marking. Mark classified E-mail messages using internal portion markings prescribed in OMB/ISOO Directive No. 1. Mark all classified E-mail messages with an overall classification. The overall classification mark must reflect the highest classification of the information contained within the entire E-mail transmission--to include all attachments. Mark all paragraphs and subparagraphs with their classification in the same manner as normal correspondence. **Attachment**

2, **Attachment 3**, and **Attachment 4** contain detailed procedures for marking classified E-mail messages and attachments.

9.5.2. Safekeeping.

9.5.2.1. Use electronic delivery receipts when transmitting classified information off the installation or to non-Air Force activities.

9.5.2.2. Confirm a person's clearance by completing one of the following:

9.5.2.2.1. Check the person's access on the Automated Security Clearance Approval System (ASCAS) roster (this only applies to Air Force employees).

9.5.2.2.2. Check the person's clearance with the employee's security manager, supervisor, or commander.

9.5.2.2.3. Check the clearance level against a valid visit request from the visitor's security manager or supervisor. See AFI 31-401, *Managing the Information Security Program*, for further guidance.

9.5.3. Declassification. Classified E-mail must contain declassification or downgrading instructions at the end of the message text. See AFI 31-401 for additional guidance.

9.5.4. Destruction of Classified E-mail.

9.5.4.1. Holders of classified E-mail must destroy it when it is no longer required. If the classified E-mail is an official record, destroy it only after the retention period in AFMAN 37-139 has expired. See Air Force Systems Security Instruction (AFSSI) 5102, *The Air Force Computer Security (COMPUSEC) Program* (will convert to AFI 33-202). For paper E-mail products, consult AFI 31-401.

9.5.4.2. Top Secret Control Officers (TSCO) use AF Form 143, **Top Secret Register Page**, or another approved form (for example, AF Form 310, **Document Receipt and Destruction Certificate**) to record the destruction of Top Secret E-mail. Attach the form to the Top Secret register page.

9.5.4.3. When you must keep a record of destroyed Secret and Confidential materials, choose from AF Form 310, or AF Form 1565, **Entry, Receipt, and Destruction Certificate** (for document page changes).

9.5.4.4. Personnel destroy residual classified information by purging or destroying electronic media in accordance with AFSSI 5020, *Remanence Security* (will convert to AFMAN 33-224).

9.5.5. Transmission Guidelines. When transmitting classified information via E-mail, take special care to transmit only that level of classified information for which the system is authorized (see **Attachment 3** and **Attachment 4**).

9.6. Handling Unclassified E-mail.

9.6.1. Special Handling Requirements. Do not transmit unclassified information that requires special handling (e.g., encrypt for transmission only [EFTO]) on or to systems not approved for that purpose.

9.6.2. PERSONAL FOR Messages. Allied Communications Publication (ACP) 121, (C) *DCS Operating Procedures* (U) established the PERSONAL FOR message. General or flag officers and civilians of equivalent rank may originate PERSONAL FOR E-mail messages from organizational accounts. Protect the privacy of the message. Deliver PERSONAL FOR messages to the individual E-mail account or the designated representative's individual E-mail account. Use the format "PERSONAL FOR (recipient's name)" or "PERSONAL FOR (recipient's name) FROM (originator's name)" in the E-mail subject line.

9.6.3. Transmission Guidelines. Transmission of unclassified information on classified networks is authorized unless specifically prohibited by the network operating instructions. The guidelines listed in **Attachment 5** apply to all unclassified E-mail sent across a classified network.

10. Information Collections and Reports (ICR).

10.1. A report control symbol (RCS) number is required to collect status, summary, or statistical information from Air Force organizations via E-mail. This type of information collection is considered an internal reporting requirement. Refer to AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Inter-Agency Air Force Information Collections* (will convert to AFI 33-324), for the proper procedures for applying for an RCS number before soliciting information through E-mail.

10.2. Use of E-mail to solicit information from the public (for example, a questionnaire, customer survey, and so forth) is authorized when it is deemed in the best interest of the Air Force. The local Public Affairs Office must approve questionnaires, surveys, and interviews prior to use. However, in most cases, OMB must approve and license information collections from the public. Refer to AFI 37-124 for further guidance.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

OMB/ISOO Directive No. 1, *Classified National Security Information*

ACP 121, (C) *DCS Operating Procedures* (U)

DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*, April 1997

DoD 5200.1-R, *DoD Information Security Program*, January 1997

DoD 5200.2-R, *Personnel Security Program*, January 1987

DoDD 5200.28, *Security Requirements for Automated Information Systems (AIS)*, May 21, 1988

Joint Ethics Regulation

Joint Technical Architecture-Air Force (JTA-AF), Version 1.5

AFPD 31-4, *Information Security*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFI 10-1101, *Operations Security*, May 1997

AFI 31-401, *Managing the Information Security Program*

AFI 31-501, *Personnel Security Program Management*, 2 May 1994

AFI 33-127, *Electronic Messaging Registration and Authority*

AFMAN 33-128, *Electronic Messaging Registration*

AFI 33-129, *Transmission of Information Via the Internet*

AFI 35-205, *Air Force Security and Policy Review Program*

AFMAN 37-123, *Management of Records* (will convert to AFMAN 33-323)

AFI 37-124, *The Information Collections Reports Management Program; Controlling Internal, Public, And Interagency Air Force Information Collections* (will convert to AFI 33-324)

AFMAN 37-126, *Preparing Official Communications* (will convert to AFMAN 33-326)

AFMAN 37-127, *Air Force Standard Office Symbols* (will convert to AFMAN 33-326)

AFI 37-131, *Freedom of Information Act Program* (will convert to DoD 5400.7-R/AF Supplement)

AFI 37-132, *Air Force Privacy Act Program* (will convert to AFI 33-332)

AFI 37-138, *Records Disposition--Procedures and Responsibilities* (will convert to AFI 33-338)

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339)

AFDIR 37-135, *Air Force Address Directory* (converted to a database)

AFH 33-337, *The Tongue and Quill*

AFSSI 5020, *Remanence Security* (will convert to AFMAN 33-224)

AFSSI 5102, *The Air Force Security (COMPUSEC) Program* (will convert to AFI 33-202)

AFRFC-001, *E-mail Address Conventions*, AFCA, 20 Dec 1996

Abbreviations and Acronyms

ACP—Allied Communications Publication

AFCA—Air Force Communications Agency

AFDIR—Air Force Directory

AFH—Air Force Handbook

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFSSI—Air Force Systems Security Instruction

ASCAS—Automated Security Clearance Approval System

BITS—Base Information Transfer System

CINC—Commander-in-Chief

CNWDI—Critical Nuclear Weapon Design Information

CSO—Communications-Information Systems Officer

DISA—Defense Information Systems Agency

DoD—Department of Defense

DoDD—Department of Defense Directive

DMS—Defense Message System

DNS—Domain Name Service

DRU—Direct Reporting Unit

EFTO—Encrypt for Transmission Only

E-mail—Electronic Mail

FOA—Field Operating Agency

FOUO—For Official Use Only

GEOREF—Geological Reference

GM—General Manager (civilian grade system)

GS—General Schedule (civilian grade system)

ICR—Information Collections and Reports

ISOO—Information Security Oversight Office

MAJCOM—Major Command

NCC—Network Control Center

OMB—Office of Management and Budget

OPSEC—Operations Security

PCS—Permanent Change of Station

RCS—Report Control Symbol

SBU—Sensitive-But-Unclassified

SSN—Social Security Number

TCP/IP—Transmission Control Protocol/Internet Protocol

TDY—Temporary Duty

TSCO—Top Secret Control Officer

UCMJ—Uniform Code of Military Justice

Terms

Agency Designee—The first supervisor who is a commissioned officer or a civilian holding a GS-11 or higher and is in the chain of command of the employee concerned.

Communications-Information Systems Officer (CSO)—The term CSO identifies the supporting CSO at all levels. At base-level, this is the communications unit commander or the commander's designated representative. The CSO is responsible for carrying out base communications and information systems responsibilities. At MAJCOM and other activities, it is the person designated by the commander as responsible for overall management of communications-information systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol "SC" which is expanded to three and four digits to identify specific functional areas. CSOs are the accountable officers for all automated data processing equipment in their inventory.

Individual E-mail Account—An E-mail account created for and accessed by a single individual only.

Information Protection Office—Formerly C4 Systems Security Office.

Internet—An informal collection of government, military, commercial, and educational computer networks using the transmission control protocol/internet protocol (TCP/IP) to transfer information. The global collection of interconnected local, mid-level, and wide-area networks that use the internet protocol as the network layer protocol.

List-server—An electronic mailing list of individuals interested in a specific topic. Individuals subscribe to list-servers by sending an E-mail message asking to be placed on the list. Once added to the list, members will receive all messages sent to the list and may post their own messages. Messages posted to the list are sent to all other subscribers.

Naming Conventions—A method of uniquely identifying an E-mail address on a network.

News group—Internet resources by which individuals interested in a particular topic may read and post messages that are accessed, read, and responded to by other internet users. News groups are moderated (where messages are screened for appropriateness before posting by individuals in charge of the news group), or unmoderated (where all messages are posted, regardless of content).

Official E-mail—E-mail communications, including emergency communications, the Air Force has determined necessary in the interest of the Federal government.

Organizational E-mail Account—An E-mail account used to receive and send formal organizational messages. Send official correspondence that tasks an organization to an organizational account.

Organizational Message—This type of message includes command and control traffic and messages exchanged between organizational elements. These messages require release by the sending organization; the receiving organization determines its distribution. Due to their official and sometimes critical nature, such messages impose operational requirements on the communications systems. These requirements may include, but are not limited to, nonroutine precedence, guaranteed timely delivery, high availability and reliability, and a specified level or survivability.

Records—All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by any agency of the US Government under federal laws, or with the transaction of public business, and preserved or appropriate for preservation by an agency, or its legitimate successor, as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and processed documents are not included.

Record-keeping System—A record-keeping system made up of a set of policies, procedures, and equipment that are used to organize and identify files or documents to speed up their retrieval, use, and disposition.

Attachment 2

MARKING CLASSIFIED ELECTRONIC MAIL MESSAGES

A2.1. Classified Information. Mark classified E-mail messages to show the level of classification of the information contained in or revealed by it.

A2.1.1. Mark all E-mail messages on classified networks by entering the appropriate classification in parenthesis by using these symbols: "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified, as the first marking in the "Subject" box of the message template. Following the subject, place the appropriate symbol indicating the appropriate classification of the subject itself. Do not send classified messages or mark messages as classified on an unclassified network (see **Attachment 5**).

A2.1.2. Place the appropriate classification of the E-mail transmission in all uppercase letters as the first line of the E-mail message text. Include no other information on this line.

A2.1.3. Begin the text of the message on the third line (that is, leave one blank line between the classification marking and the beginning of the E-mail message text).

A2.1.4. Use abbreviated classification symbol at the beginning of all paragraphs and subparagraphs.

A2.1.5. Place the appropriate classification of the E-mail transmission in all uppercase letters as the last line of the E-mail text. Include no other information on this line.

A2.1.6. Indicate the security classification of any attachments by placing the abbreviated classification symbol in parentheses before the attachment icon. If the E-mail message is unclassified without the attachments, then add this mandatory line: "THIS MESSAGE IS UNCLASSIFIED WHEN SEPARATED FROM ATTACHMENT."

A2.1.7. Place Critical Nuclear Weapon Design Information (CNWDI), Cryptographic, Restricted Data, or other designators indicating special handling in the text following the security classification. Place markings for RESTRICTED DATA-ATOMIC ENERGY ACT 1954, and FORMERLY RESTRICTED DATA ATOMIC ENERGY ACT on the message as shown in DoD Pamphlet 5200.1-PH, *DoD Guide to Marking Classified Documents*, April 1997; AFPD 31-4, *Information Security*; and AFI 31-401.

A2.2. Reply and Forward Actions:

A2.2.1. Reply and forward actions carry the highest classification of any information contained within the appended E-mail transmissions.

A2.2.2. Text markings included in a "Reply/Forward" will follow instructions listed above.

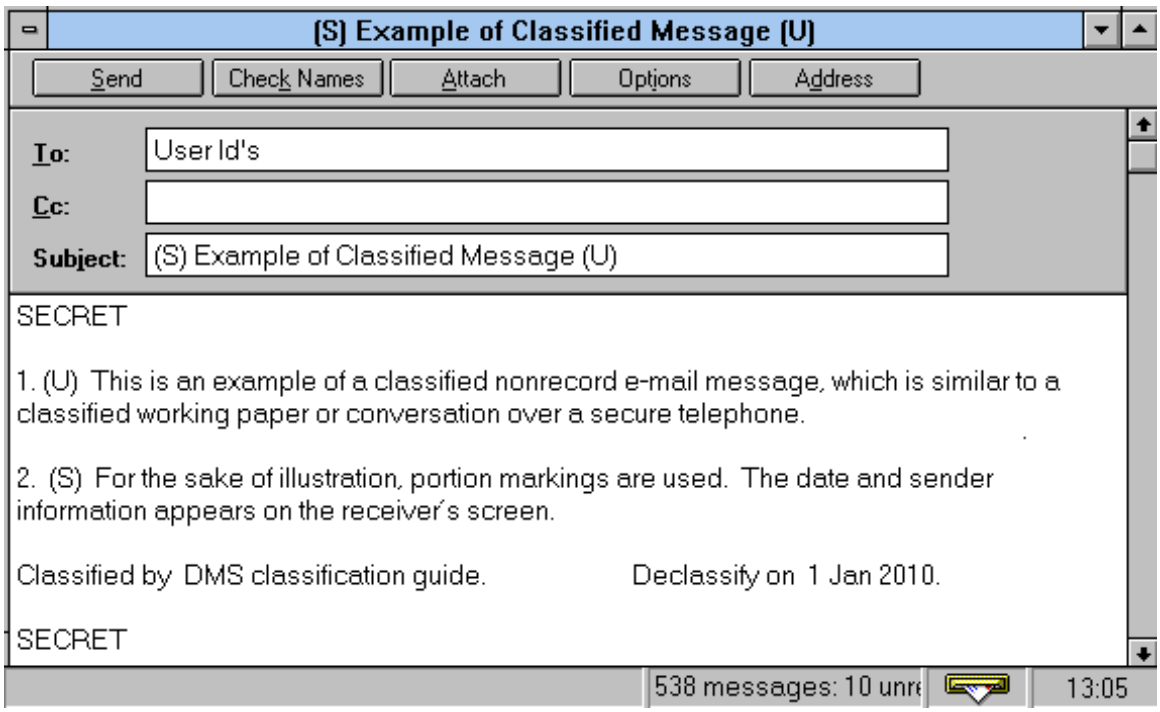
A2.2.3. If comments included in a "Reply/Forward" change the classification level of the E-mail transmission, then change the classification symbol of the "Subject" box and message text markings accordingly.

Attachment 3

TRANSMITTING CLASSIFIED MESSAGES AND ATTACHMENTS

A3.1. Transmitting Classified Messages and Attachments. **Figure A3.1.** is unclassified; security markings are for instructional purposes only.

Figure A3.1. Example of Classified E-mail Message.



NOTES:

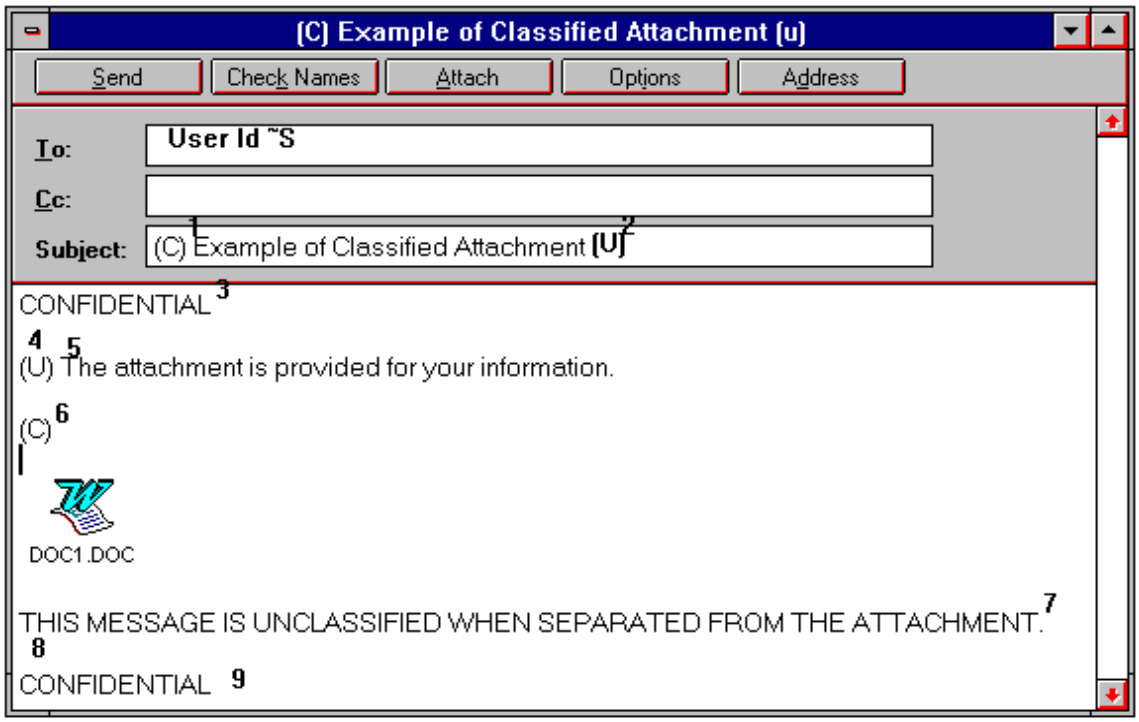
1. Subject Line, First Entry: Appropriate classification symbol for the overall classification of E-mail transmission.
2. Subject classification symbol (classified message).
3. Text Box, First Line: Overall classification of E-mail message and attachments.
4. One blank line between classification and message text.
5. Paragraph classification symbols (classified message).
6. One blank line between text and classification.
7. Classified by and declassification or downgrading instructions
8. Last Line of Text: Overall classification.

Attachment 4

ATTACHING A CLASSIFIED ATTACHMENT

A4.1. Attaching a Classified Attachment. **Figure A4.1.** is unclassified; security markings are for instructional purposes only.

Figure A4.1. Example of E-mail Message with Classified Attachment.



NOTES:

1. Subject Line, First Entry: Appropriate classification symbol for the overall classification of E-mail transmission.
2. Subject classification symbol (classified message).
3. Text Box, First Line: Overall classification of E-mail message and attachments.
4. One blank line between classification and message text.
5. Paragraph classification symbols (classified message).
6. Attachment classification symbol.
7. Caveat for classification when E-mail message is separated from the attachment.
8. One blank line between text and classification.
9. Last Line of Text: Overall classification.

Attachment 5

TRANSMITTING UNCLASSIFIED INFORMATION ON CLASSIFIED NETWORKS

A5.1. Transmitting Unclassified Information on Classified Networks. Use the following guidelines for all unclassified E-mail sent across any network cleared for classified material (see **Figure A5.1.**):

A5.1.1. Mark unclassified E-mail messages sent across classified networks by entering the symbol "(U)" in parenthesis as the first marking in the "Subject" box of the message.

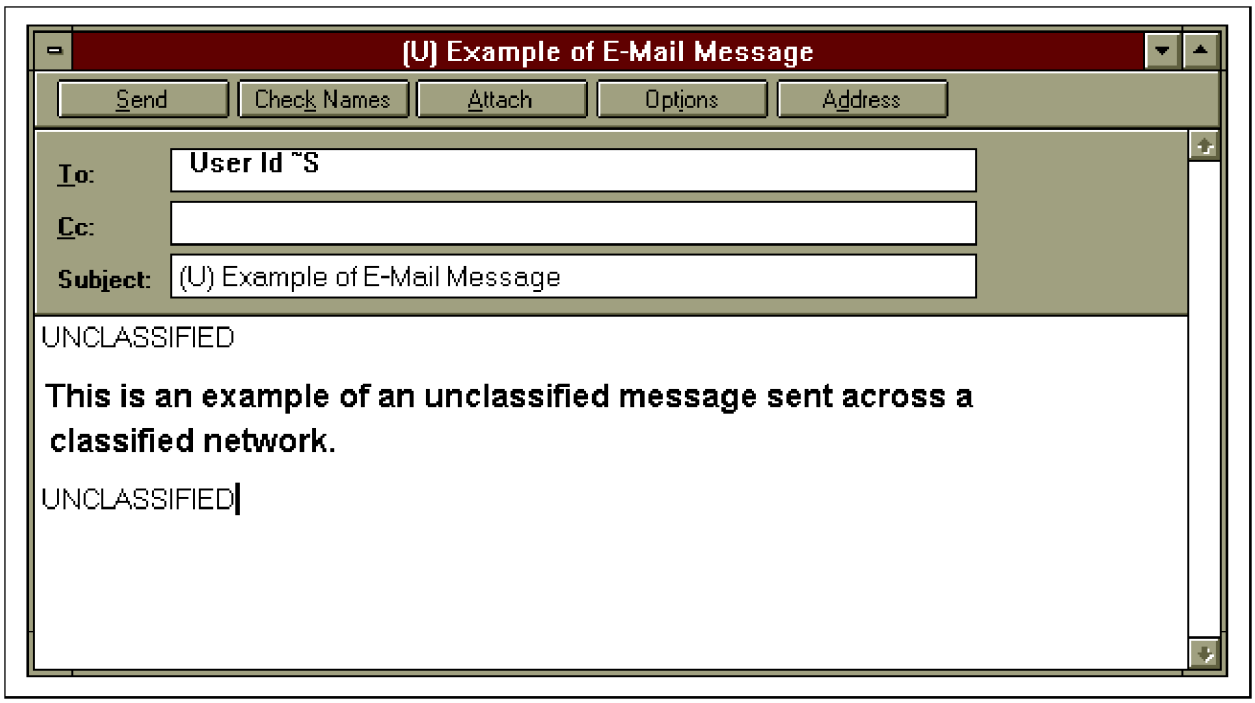
A5.1.2. Place the word UNCLASSIFIED in uppercase letters as the first line of the E-mail text. Include no other text on this line.

A5.1.3. Begin the text of the message on the third line (that is, one blank line between UNCLASSIFIED and the beginning of the E-mail message text).

A5.1.4. Place the word UNCLASSIFIED in uppercase letters two lines below the last line of the message text (that is, one blank line between "UNCLASSIFIED" and the last line of the E-mail message). Include no other text on this line.

A5.1.5. Attachments included in an unclassified E-mail transmission do not need to have the classification noted. ***NOTE:*** If an attachment is classified, the entire E-mail transmission is classified.

Figure A5.1. Example of Unclassified E-mail Sent Across a Classified Network.



Attachment 6

ELECTRONIC MAIL (E-MAIL) NAMING CONVENTIONS

A6.1. Purpose: Standard naming conventions are critical to the interoperability and configuration control of Air Force owned, maintained, or operated electronic messaging systems. These naming conventions apply specifically to Air Force-owned messaging systems and Air Force-operated Defense Message System (DMS) equipment. These conventions are absolutely crucial to the optimum operation of, and interoperability between, DMS-AF and non-DMS-AF sites. In the interest of clarity, the DMS-AF and recommended Air Force platforms were used to help explain these naming convention concepts. However, you should apply these naming conventions to other messaging systems as appropriate.

A6.2. Background.

A6.2.1. Follow these conventions even if you plan to keep DMS-AF and non-DMS-AF sites separated. However, the DMS-AF is considered the final E-mail environment every Air Force base will migrate to for all E-mail services. In that context, DMS-AF and non-DMS-AF sites will merge and the base will then have only a single DMS-AF site consisting of DMS-AF servers and a mix of DMS-AF and non-DMS-AF clients.

A6.2.2. Air Force E-Mail addresses are composed of two elements which are specified in the following format: [UserID]@[domain name]. Domain names will follow the formats specified in AFMAN 33-128, *Electronic Messaging Registration*.

A6.2.3. Failure to follow the mandatory naming conventions for the organization and DMS-AF servers will result in reloading servers (a significant task) in order to integrate DMS-AF with non-DMS-AF products. Failure to follow the recommended naming conventions may cause interoperability problems as Air Force-wide directory synchronization starts to occur.

A6.3. Air Force Naming Conventions.

A6.3.1. Organization Naming Convention. Set the DMS-AF and non-DMS-AF site Organization Name to read "ORGANIZATION" (spelled out in all uppercase letters) during the initial installation. Enter this name during the initial setup of the server; it cannot be changed at a later date without completely reinstalling the system. This is necessary as it enables non-DMS-AF sites to share directory, public folders, distribution lists, and group-ware applications with DMS-AF sites. Bases and organizations must conform to this convention prior to DMS-AF implementation on the base.

A6.3.2. Site Naming Convention. The DMS-AF site name is not used by any outside resource or service. All organizations must use site names that are unique within their organization. Spell out the main DMS-AF site name in upper case (e.g., LANGLEY). This is the same convention recommended for the base NT Domain and the Domain Name Server (DNS). If this convention was already used as a non-DMS-AF site name, then the DMS-AF site should choose an alternate site name of "SITENAME AFB" (e.g., LANGLEY AFB).

A6.3.3. Primary Server Naming Convention. The DMS-AF primary (e.g., ESL® Primary, Lotus® Hub, and Microsoft® Bridgehead) server and its backup must conform to the 8-character naming convention specified in the DMS Sub Registration Authority (SRA) Document. This is because DMS uses this convention in its management procedures. All other local servers (DMS-AF and non-DMS-AF) should also use the 8-character naming convention as specified in the DMS SRA doc-

ument or use the AFCA-recommended server naming conventions (i.e., emh1, emh2, emh3, emhx) as specified in AFRFC-001, *E-mail Address Conventions*, AFCA, 20 December 1996. ***NOTE:*** Ensure the server host name is the same as the system's NETBIOS name, the NT server name, and the DNS name. The DMS 8-character naming convention as specified in the DMS SRA document is as follows:

A6.3.3.1. The first position is a 1-character service/agency code (upper case) representing the maintenance provider (i.e., K for DISA-purchased servers, F for Air Force-purchased servers).

A6.3.3.2. The second position is a 1-character code (upper case) representing the type of DMS component (i.e., servers are always S).

A6.3.3.3. The next four positions contain a 4-character code (upper case) conforming to the DCAC 310-65-1, Chapter 33, geological reference (GEOREF) code. This authoritative source identifies the physical location of the server. These codes are available at the following web site: http://www.ssg.gunter.af.mil/dms/library/reference/georef.htm.

A6.3.3.4. The last two positions contain a 2-character code used to identify a specific server at a location. The code 01 is reserved for use as the DMS sensitive-but-unclassified (SBU) primary server and 02 is reserved for use as the DMS SBU backup server. The SECRET community will use 76 and 77 as the primary and backup server identification codes, respectively. Use a base 34 number (X_{34}) if you need to identify more than 99 servers. Obtain the X_{34} number by using a combination of 10 numbers (i.e., 0 - 9) and 24 letters (i.e., A - K, M, N, and P - Z; the letters L and O are reserved--do not use them).

Example: A non-DMS AF server on Gunter AFB would be named "FSJUBJ04." Where F = Air Force-purchased and maintained, S = server, JUBJ = Gunter AFB GEOREF code, and 04 = the sequential identification number of the server.

A6.3.4. Public Folder Naming Convention. Only the base name in the following format should be used at the top level: <base AFB> (e.g., Langley AFB). Failure to adhere to this convention will cause replication and possibly conflicting folder names. Below the base name, there is no set format. This issue requires further study to determine if there is some benefit to establishing standard lower-level folder names which bases should adhere to. Standard public folders offer a tremendous potential to streamline AF-wide business processes used to coordinate and act on official correspondence.

A6.4. X.400 Protocol & X.500 Standard Conventions.

A6.4.1. Originator/Recipient (O/R) Address. Use the DMS SRA format listed below to fill in the O/R address string variables:

/s=lastname/g=firstname/i=middleinitial/q=generationqualifier/o=ST1/ou1=georefcode##/c=us/a=DMS.

A6.4.1.1. A breakout of the O/R address string is listed below to help clarify the meaning and intent of each individual variable contained in the O/R address shown in **Table A6.1.**

Table A6.1. Breakout of O/R Address String.

s = last name (surname)
g = first name (given name)
i = middle initial
q = generation qualifier (i.e., Jr., I, II, III, etc)
o = ST1 (i.e., two letter state abbreviation and # is a sequence number)
ou1 = geographic reference code number (georefcode##)
c = us
a = DMS

A6.4.1.2. Keep this address the same as the DMS X.500 O/R address so users can access the DMS directory. The system administrator will set the server to default to this convention.

A6.4.1.3. Ensure the X.400 address is correct. The X.400 address screen display should yield the surname (s), given name (g), middle initial (i), and generation qualifier (q). Only display those portions of the name which were included during the creation of the mailbox. Leave the Common Name block blank.

A6.4.1.4. Set the defaults for the "o" and "ou1" values to o=ST# where ST is the two-letter state abbreviation and # is a sequence number. Set "1" as the first location in the state and subsequent sites will have higher numbers. The ou1=XXXX## where the XXXX is the four-character geographical reference code and the ## is once again a sequence number based on the number of DMS X.400 message transfer agent addresses at a given location.

A6.4.1.5. The c=US and ADMD=DMS values are automatic defaults for DMS servers and are created when the X.400 connector is created during the entry of DMS users.

A6.4.2. O/R Address. Use the format specified in the DMS SRA to define the X.500 address in the DMS Directory Information Tree (DIT). Ensure the X.500 O/R address is the same as the X.400 O/R address or the DMS User Agent (client) cannot process military elements of service (P42/P772) messaging. This is a common cause of failure in creating new DMS users.

A6.4.3. Common Name (CN). The CN is used in the DMS Directory Information Tree (DIT). All non-DMS sites should follow this convention during the creation of non-DMS accounts. Once DMS is implemented the format becomes mandatory. The format for this field is specified in the DMS SRA and can be service-unique. The Air Force standard is last name, first name, middle initial, and rank. Punctuation, including commas, is not allowed, thus its syntax is: <LastName FirstName MiddleInitial rank>. For example, Deere John D 2Lt. The CN cannot exceed 64 characters in length. Individuals with no middle initial should have the middle initial field left blank; do not use the no-middle-initial (NMI) abbreviation. Use "Contractor" in the rank field to identify vendors and contractors. See **Table A6.2.**

A6.4.4. Organizational Display Naming Convention. The recommended format for the organizational display name conforms to the DMS X.500 organization common name convention as identified in the DMS SRA document. Punctuation (including commas) is not permitted between the elements, thus its syntax is: <Org/Office short description of office> (e.g., ACC/SE Safety Office).

A6.4.5. Individual Display Naming Convention. This individual display name format is required to preposition the Air Force for future directory synchronization and standardization efforts. The standard Air Force naming convention is last name, first name, middle initial, generation qualifier, rank, organization, and office. Punctuation (including commas) is not permitted between the elements, thus its syntax is: <LastName Firstname MiddleInitial GenerationQualifier Rank Organization/Office>. Use "Contractor" in the rank field to identify vendors and contractors. See **Table A6.2.** If a tie-breaker is needed, use the middle name spelled out (e.g., Smith Joe Ernest Jr TSgt ACC/SCB). If a tie still exists, then the rank, organization, and office should uniquely identify an individual.

A6.4.6. Alias Naming Convention. Use the same alias as the UserID portion of the SMTP address convention (firstname**.**lastname). For example John Smith is represented by john**.**smith. The system administrator should set the alias to default to this convention. Whatever appears in the alias field will automatically create the default SMTP address.

A6.5. SMTP Conventions.

A6.5.1. SMTP Organization Naming Convention. An organizational E-Mail account must use a combination of the standard organizational abbreviation and standard Air Force office symbol to form the UserID. Obtain the standard organizational abbreviation from AFDIR 37-135, *Air Force Address Directory* (converted to a database at http://afdir.hq.af.mil/afdir/index.cfm). Obtain the standard Air Force office symbol from AFMAN 37-127, *Air Force Standard Office Symbols* (will convert to AFMAN 33-326).

A6.5.1.1. The format for the SMTP organization naming convention is Org**.**Office@base**.**af**.**mil. For example, HQ SSG/LG is represented as SSG**.**LG@gunter**.**af**.**mil. The preceding HQ is not used.

A6.5.1.2. UserIDs for units at wing, group, and squadron level will consist of the standard organizational abbreviation and standard Air Force office symbols separated by a period. For example, the Commander, 10th Wing, is represented as 10WG**.**CC and the Commander, 10th Communications Group, is represented as 10CG**.**CC. You may add additional information as needed to accommodate other units such as detachments and operating locations: For example, the Commander, Detachment 1, 10th Wing, is represented as 10WG**.**DET1**.**CC.

A6.5.1.3. UserIDs for higher headquarters will consist of the headquarters standard organizational abbreviation and standard Air Force office symbol separated by a period (for example, USAF**.**SCXX and SAF**.**AAD).

A6.6. SMTP Individual Naming Convention. The SMTP naming convention is predicated on two concepts. First, a base has a single messaging environment that maps into the base DNS. Second, the messaging system is not limited to an 8-character UserID. However, in the interest of flexibility, the naming convention for an 8-character UserID system is also included below:

A6.6.1. The format for "Individual" SMTP addresses is <firstname**.**lastname@base**.**af**.**mil>. For example, Paul Armel is represented as paul**.**armel@pentagon**.**af**.**mil. Hyphenated names, like Becky Easton-Jones becomes becky**.**easton-jones. Add a period and a number as needed to specifically identify users with similar names within domains. For example, you would represent a second person named Jane Smith as jane**.**smith**.**2@moody**.**af**.**mil. Single quotes in names are not permitted, thus

"Scott O'Grady" becomes scott**.**ogrady. This format conforms to the preferred Air Force NT network operating system login name and Air Force-wide remote access UserID.

A6.6.2. For nonstandard systems, limited to an 8-character UserID, use the last name only. If more than one person has the same last name, append the last name with a number (for example: smith, smith2, smith3,Ösmithx). Limit last names to eight characters (for example, burkowitz becomes burkowit). If more than one person has the same last name and the last name exceeds eight letters, limit the name to seven characters and add a number. For example, the first burkowitz becomes burkowit. Subsequent burkowitzs' become burkowi1, burkowi2, burkowi3, etc.

A6.7. SMTP Alias Naming Convention. There is flexibility for a user whose common name is different than his/her first name. The E-Mail system administrator can add a second SMTP address of <common-firstname**.**lastname@base**.**af**.**mil>. The end result for a user "Robert Smith" whose common name is "Bob Smith" is an NT Login ID of <Robert**.**Smith>, an Exchange alias of <Robert**.**Smith>, a primary SMTP address of <Robert**.**Smith> (for replies,) and a secondary SMTP address of <Bob**.**Smith>.

Table A6.2. Air Force Rank Naming Convention.

Enlisted	**Officer**	**Air Force/DoD Civilian** (Where ## = grade)	**Contractor**
AB	2Lt	WS-##	Contractor
Amn	1Lt	GS-##	
A1C	Capt	GM-##	
SrA	Maj	SES-##	
SSgt	LtCol		
TSgt	Col		
MSgt	BrigGen		
SMSgt	MajGen		
CMSgt	LtGen		
	Gen		